PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 12/22, 29/06, H04Q 7/22, H04L 12/56

A1

(11) International Publication Number: **WO 99/59293**

(43) International Publication Date: 18 November 1999 (18.11.99)

(21) International Application Number: PCT/SE99/00686

(22) International Filing Date: 27 April 1999 (27.04.99)

(30) Priority Data:
09/078,447 13 May 1998 (13.05.98) US

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S–126 25 Stockholm (SE).

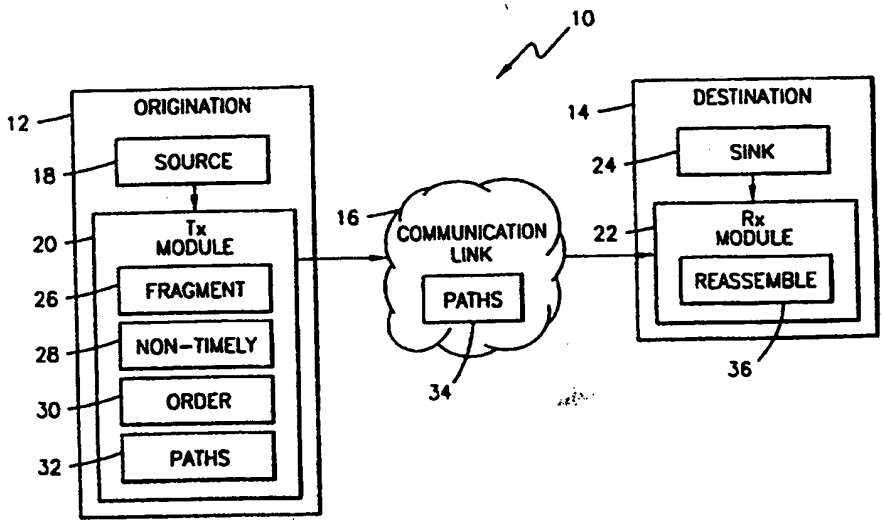
(72) Inventors: MALETTE, Louis; 528 Joseph Bonnet, St–Eustache J7R 5E1 (CA). BUGNON, Jacques; 12 Plateau Belmont, Repentigny J6A 3N9 (CA).

(74) Agent: ERICSSON RADIO SYSTEMS AB; Common Patent Dept., S–164 80 Stockholm (SE).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: DATA TRANSFER METHOD WITH VARYING PACKET TRANSMISSION TIME INTERVAL SECURITY PROTOCOL



(57) Abstract

A message to be communicated over an unsecure communications link (16) is fragmented (26) into a plurality of packets (each of perhaps varying length). The packets are then individually transmitted (20) over the unsecure communications link with an introduced varying (perhaps, randomly or pseudo–randomly) selected inter–packet time interval (delay). Received packets are then reassembled (36) to regenerate the original message. To provide enhanced security against eavesdropping, the packets are not only transmitted in a non–timely manner (28) with the inter–packet time delay, but are also either routed (32) over different transmission paths (34) supported by the communications link or disordered (30) in a random or pseudo–random manner prior to transmission.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

DATA TRANSFER METHOD WITH VARYING PACKET TRANSMISSION TIME INTERVAL SECURITY PROTOCOL

BACKGROUND OF THE INVENTION

Technical Field of the Invention

The present invention relates to a method and system for providing secure communications and, in particular, to a method and system for splitting a sensitive message to be communicated into plural packets (perhaps having variable lengths) and then transmitting the individual packets from a source to a destination with a selected varying time interval between successive packets.

Description of Related Art

More and more frequently, users have a need to communicate sensitive information over unsecure communications links. Many sophisticated scrambling and encrypting techniques have been developed to support secure communications efforts in such environments. These sophisticated techniques are often times quite complex procedures. There may also be sizeable monetary expense associated with the implementation of these techniques. In many instances, such sophisticated techniques provide an "over-engineered" and too expensive solution to the concern of deterring eavesdropping. What is needed is a more suitable solution (from both a complexity and expense perspective) that provides some deterrence protection against third party eavesdropping on communications messages transmitted over unsecure communications links.

SUMMARY OF THE INVENTION

A message to be communicated over an unsecure communications link is fragmented into a plurality of packets. These individual packets may, if desired, have varying lengths. A transmitter module then individually transmits the packets over the unsecure communications link. The transmissions of the individual packets are made by the module in such a fashion as to introduce a varying (perhaps, randomly or pseudo-randomly) selected inter-packet time interval (delay) between successive packets. At a receiver module, the transmitted packets are received and reassembled to regenerate the original message. This protocol for non-timely transmission of the individual message packets serves to make it more difficult for an eavesdropper to capture all of the message packets and reconstruct the transmitted message. Enhanced security is provided by not only transmitting the packets in a non-timely manner, but

also by either sending the packets over different transmission paths supported by the communications link or disordering the packets in a random or pseudo random manner prior to transmission.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the method and apparatus of the present invention may be acquired by reference to the following Detailed Description when taken in conjunction with the accompanying Drawings wherein:

FIGURE 1 is a block diagram of a communications system implementing a security protocol in accordance with the present invention; and

FIGURE 2 is a flow diagram illustrating a method of operation concerning the security protocol of the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

Reference is now made to FIGURE 1 wherein there is shown a block diagram of a communications system 10 implementing a security protocol in accordance with the present invention. The communications system 10 includes an origination node 12 and a destination node 14 interconnected for communication by a communications link 16. The origination node 12 includes a source 18 for generating message traffic. The source 18 generated messages are then handled by a transmitter module 20 for transmission over the communications link 16 towards the destination node 14. A receiver module 22 in the destination node 14 receives the transmitted messages, and outputs the messages to a message sink 24.

The transmitter module 20 includes a first functionality 26 for taking a message received from the source 18 and fragmenting the message into a plurality of individual packets. The fragmenting process may, if desired, generate individual packets of varying, rather than consistent, lengths. The transmitter module 20 then utilizes a second functionality 28 for transmitting the generated individual packets in a non-timely fashion. By "non-timely" it is meant that the individual packets are transmitted by the transmitter module 20 over the communications link 16 with a varying inter-packet time interval (delay) between successive packets in the source originated message. This introduced delay between packets may be of either a randomly or pseudo randomly selected duration. The introduced varying inter-packet time delay serves to enhance the security of packet transmission over the communications link 16 as a potential eavesdropper does not know when each of the successive packets comprising the complete message are to be transmitted. Delays may be selectively chosen (from packet to packet) in a variable range from as short as

a few milliseconds to as long as a few minutes. Even longer delays (on the order of hours or days) providing for even more secure message communication may be specified and implemented by the functionality 28 for use in situations where communication of the original message is not time-sensitive in nature. To provide for even more secure message communication, a third and a fourth functionality, 30 and 32, respectively, are selectively implemented in conjunction with the non-timely transmission functionality 28. The third functionality 30 further introduces a random or pseudo random disordering of the message packets prior to non-timely transmission over the communications link 16. The fourth functionality 32 further introduces the transmission of the individual packets over different ones of a plurality of communications paths 34 supported by the communications link 16. In this regard, the paths 34 may comprise different logical or physical channels within the communications link 16.

The receiver module 22 includes a message reassembly functionality 36 for receiving the non-timely transmitted packets (perhaps in either or both a disordered manner and/or from different paths 34), and then coordinating the reconstruction of the original message as generated by the source 18. The reconstructed message is then output by the functionality 36 to the sink 24 for further processing and handling. The functionality 36 includes appropriate memory (not shown) for temporarily caching received message packets prior to processing and completion of the message reconstruction action.

In a specific implementation of the present invention, the system 10 comprises a telecommunications system, the origination node 12 sends a message on behalf of a user (such as a user mobile station), the destination node 14 comprises a network communications node (such as a mobile switching center or home location register), and the communications link 16 comprises a signaling network of the telecommunications system. In this implementation, the message being communicated in a fragmented, non-timely manner may comprises sensitive telecommunications information such as authentication data. The secure transmission protocol of the present invention accordingly provides a level of defense against the interception of this sensitive mobile station information and possible cloning of the mobile station.

Reference is now made to FIGURE 2 wherein there is shown a flow diagram illustrating a method of operation concerning the security protocol of the present invention. In step 100, a message is originated for transmission. In step 102, that originated message is fragmenting into a plurality of individual packets. The fragmenting process of step 102 may, if desired, generate individual packets of

varying, rather than consistent, lengths. Next, in step 104, the generated individual packets are optionally disordered in either a random or a pseudo random manner. The generated individual packets are then transmitted in step 106 in a non-timely fashion such that there is introduced between the transmission of individual packets a randomly or pseudo randomly varying inter-packet time interval (delay). The non-timely transmission of step 106 may further involve selectively transmitting the individual packets over different ones of a plurality of communications paths (such as plural physical or logical channels). In step 108, the non-timely transmitted packets are received. Reassembly of the packets back into the original message occurs in step 110. This step of reassembly in step 110 accounts not only for the introduced inter-packet time delay, but also for any optionally introduced variance in packet size, packet disordering or differences in transmission path. The regenerated message is then output in step 112.

Although preferred embodiments of the method and apparatus of the present invention have been illustrated in the accompanying Drawings and described in the foregoing Detailed Description, it will be understood that the invention is not limited to the embodiments disclosed, but is capable of numerous rearrangements, modifications and substitutions without departing from the spirit of the invention as set forth and defined by the following claims.

WHAT IS CLAIMED IS:

1. A communications method, comprising the steps of:

generating a message to be communicated;

fragmenting the generated message into a plurality of message packets;

transmitting each of the plurality of message packets comprising the message individually with a varying inter-packet transmission time interval;

receiving the individually transmitted message packets; and

reassembling the message from the received message packets.

2. The method as in claim 1 wherein the varying inter-packet transmission time interval is randomly or pseudo randomly selected.

3. The method as in claim 1 wherein the step of fragmenting comprises the step of fragmenting the message into a plurality of message packets having variable lengths.

4. The method as in claim 1 further including the step of disordering the plurality of message packets prior to transmission.

5. The method as in claim 4 wherein the step of disordering introduces a random or pseudo random shuffling of the message packets comprising the message.

6. The method as in claim 1 wherein the step of transmitting further includes the step of transmitting the plurality of message packets over different ones of a plurality of communications paths.

7. The method of claim 6 wherein the plurality of communications paths comprise plural physical channels.

8. The method of claim 6 wherein the plurality of communications paths comprise plural logical channels.

9. A communications system, comprising:

a communications link;

an origination node connected to the communications link and including functionality for fragmenting a message into a plurality of message packets and transmitting each of the plurality of message packets comprising the message

individually over the communications link with a varying inter-packet transmission time interval; and

a destination node connected to the communications link and receiving the transmitted message packets, the destination node including functionality for reassembling the message from the received message packets.

10. The system as in claim 9 wherein the functionality of the origination node introduces a randomly or pseudo randomly selected varying inter-packet transmission time interval.

11. The system as in claim 9 wherein the functionality of the origination node fragments the message into a plurality of message packets having variable lengths.

12. The system as in claim 9 wherein the functionality of the origination node further disorders the plurality of message packets prior to transmission.

13. The system as in claim 12 wherein the disordering introduces a random or pseudo random shuffling of the message packets comprising the message.

14. The system as in claim 9 wherein the functionality of the origination node for transmitting further transmits the plurality of message packets over different ones of a plurality of communications paths.

15. The system of claim 14 wherein the plurality of communications paths comprise plural physical channels.

16. The system of claim 14 wherein the plurality of communications paths comprise plural logical channels.

17. The system as in claim 9 wherein the system comprises a mobile telecommunications system, the origination node transmits mobile station related sensitive information, the destination node comprises a network communications node, and the communications link comprises a mobile telecommunications signaling network.

18. The system of claim 17 wherein the message contains mobile station authentication related information.

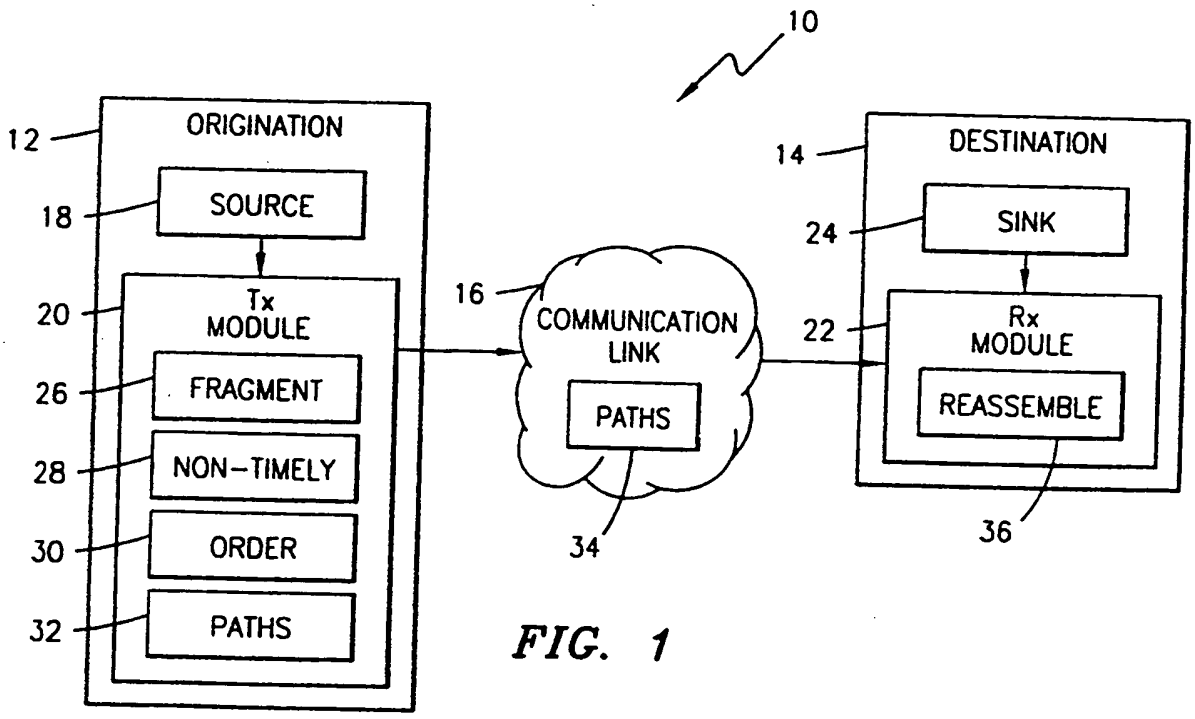

10
12
ORIGINATION
18
SOURCE
20
Tx
MODULE
26
FRAGMENT
28
NON-TIMELY
30
ORDER
32
PATHS
16
COMMUNICATION
LINK
PATHS
34
14
DESTINATION
24
SINK
22
Rx
MODULE
REASSEMBLE
36

FIG. 1

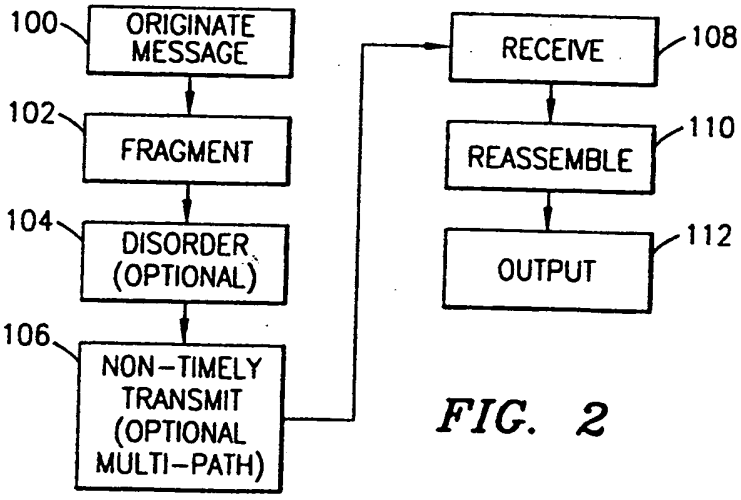

100
ORIGINATE
MESSAGE
102
FRAGMENT
104
DISORDER
(OPTIONAL)
106
NON-TIMELY
TRANSMIT
(OPTIONAL
MULTI-PATH)
RECEIVE
108
REASSEMBLE
110
OUTPUT
112

FIG. 2

INTERNATIONAL SEARCH REPORT

Interr nal Application No
PCT/SE 99/00686

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L12/22 H04L29/06 H04Q7/22 H04L12/56

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L H04Q G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4 761 778 A (HUI JOSEPH Y N) 2 August 1988 (1988-08-02) abstract column 2, line 43 - line 68	1,2,9,10
Y	column 4, paragraph 25 - paragraph 53; claim 1	3-8, 11-16

Y	US 5 680 400 A (YORK KENNETH L) 21 October 1997 (1997-10-21) abstract	3,6-8, 11,14-16
A	column 1, line 45 -column 5, line 17	1,9

Y	EP 0 830 017 A (NEXTLEVEL SYSTEMS INC) 18 March 1998 (1998-03-18) abstract	4,5,12, 13
A	page 3, line 3 - line 26 page 3, line 56 - line 58 page 5, line 23 -page 6, line 31	1,9

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 October 1999	05/11/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Karavassilis, N

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interr' nal Application No
PCT/SE 99/00686

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 98 10561 A (ERICSSON TELEFON AB L M) 12 March 1998 (1998-03-12) the whole document -----	17,18

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

...rmation on patent family members

Internr ...al Application No
PCT/SE 99/00686

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4761778 A	02-08-1988	JP 61281648 A	12-12-1986
US 5680400 A	21-10-1997	NONE	
EP 0830017 A	18-03-1998	AU 3761497 A	19-03-1998
		CA 2215874 A	17-03-1998
		JP 10294767 A	04-11-1998
		NO 974091 A	18-03-1998
WO 9810561 A	12-03-1998	US 5850444 A	15-12-1998
		AU 3955697 A	26-03-1998
		EP 0923827 A	23-06-1999